



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/675,399	09/29/2000	Carl Bilicska	Bilicska 3-2	9208

7590

12/05/2005

HARNESS, DICKEY & PIERCE, P.L.C.  
P.O. BOX 8910  
RESTON, VA 20195

EXAMINER

MAHMOUDI, HASSAN

ART UNIT

PAPER NUMBER

2165

DATE MAILED: 12/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/675,399	<b>Applicant(s)</b> BILICKA ET AL.	
	<b>Examiner</b> Tony Mahmoudi	<b>Art Unit</b> 2165	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 23 September 2005.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,2,4,6-11,13 and 14 is/are rejected.
- 7) ☒ Claim(s) 3,5 and 12 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 June 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **D ETAILED ACTION**

### ***Remarks***

1. In response to communications filed on 23-September-2005, claims 1-14 are presently pending in the application, of which, claims 1 and 9 are presented in independent form.

### ***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that said subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-2, 4, 6-11, and 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reed et al (U.S. Patent No. 5,862,325) in view of Ramasubramani et al (U.S. Patent No. 6,233,577B1.)

As to claim 1, Reed et al teaches an automated (see Abstract) authentication handling system (see column 26, lines 12-15) for use by clients (see column 26, lines 15-16) on a network (see Abstract, and see column 27, lines 62-64) comprising:

an authentication server (see column 97, line 60 through column 98, line 1) adapted to establish a two-way communication link (see column 76, lines 34-44, and see column 81, lines 59-67.)

Reed et al does not teach a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

Ramasubramani et al teaches a centralized certificate management system (see Abstract), in which he teaches a two-way (see column 3, lines 20-22, and see column 5, lines 3-5) trusted communication link (see column 3, lines 48-52, and see column 6, lines 34-38) for access by an authenticated user to a list of application servers associated with a client identifier (see Abstract, where “list of application servers” is read on “plurality of secure servers”, see column 7, lines 41-45, where “authenticated user” is read on user with a created account, and “list of application servers” is read on “certain web servers”, also see column 8, lines 17-49, and see column 14, lines 6-25.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reed et al to include a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reed et al by the teaching of Ramasubramani et al, because including a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier, would enable the system to provide secure means for authenticated clients for accessing desired web sites hosted by

Art Unit: 2165

various servers throughout a network. For example, the system can establish a two-way trusted (secured) communications link between authenticated users (shoppers) and various e-Commerce merchants, in which, the authenticity of the message and identity of the shopper (sender) would be validated by the merchant, as taught by Ramasubramani et al (see column 4, lines 18-28.)

As to claim 2, Reed et al as modified teaches wherein the authentication server (see Reed et al, column 97, line 60 through column 98, line 1) includes:

an identification engine configured to maintain collections of session assignments for accessing the application servers, each of the session assignment collections being associated with the client identifier (see Reed et al, column 26, lines 36-46, where “identification engine” is read on “system ID assignment function”, “maintain collection of session assignments” is read on “control the access”, also see Ramasubramani et al, column 8, lines 7-49.)

As to claim 4, Reed et al as modified teaches wherein the authentication server (see Reed et al, column 97, line 60 through column 98, line 1) includes:

a communication initiator engine (see Reed et al, column 109, lines 19-28) configured to establish the trusted communication link between the authenticated users and an application server (see Reed et al, column 97, line 63 through column 98, line 1; column 100, lines 52-57; and see column 107, lines 44-51) on the list (see Ramasubramani et al, column 7, lines 41-45, where “list of application servers” is read on “certain web servers”).

As to claim 6, Reed et al as modified teaches wherein the session assignments include data fields (see Reed et al, column 67, line 64 through column 68, line 3) selected from the group consisting of session timeout and application access level (see Reed et al, column 70, line 63 through column 70, line 10.)

As to claim 7, Reed et al as modified teaches wherein the client identifier includes a user id and password (see Reed et al, column 72, lines 22-42, and see Ramasubramani et al, column 7, lines 10-16.)

As to claim 8, Reed et al as modified teaches wherein the authentication includes a processor under the control of software (see Reed et al, column 13, lines 7-12) to:

receive an authentication signal from the client (see Reed et al, column 28, lines 25-37);  
provide an application access interface to the client in response to the authentication signal (see Reed et al, figures 22-24); and

establish the trusted communication link between the client and an application server selected from the application access interface (see Reed et al, column 100, lines 52-57, and see column 107, lines 44-51, and see Ramasubramani et al, column 3, lines 48-52, and see column 6, lines 34-38.)

Art Unit: 2165

As to claim 9, Reed et al teaches a method for automatically authenticating a client (see column 26, lines 12-15) for a plurality of application servers (see column 9, lines 50-65, and see column 25, lines 15-18) comprising the steps of:

providing an authentication server (see column 97, line 60 through column 98, line 1);

identifying clients for access to the application servers by the authentication server (see column 78, lines 25-32); and

Reed et al does not teach a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

Ramasubramani et al teaches a centralized certificate management system (see Abstract), in which he teaches a two-way (see column 3, lines 20-22, and see column 5, lines 3-5) trusted communication link (see column 3, lines 48-52, and see column 6, lines 34-38) for access by an authenticated user to a list of application servers associated with a client identifier (see Abstract, where “list of application servers” is read on “plurality of secure servers”, see column 7, lines 41-45, where “authenticated user” is read on user with a created account, and “list of application servers” is read on “certain web servers”, also see column 8, lines 17-49, and see column 14, lines 6-25.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reed et al to include a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reed et al by the teaching of Ramasubramani et al,

Art Unit: 2165

because including a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier, would enable the system to provide secure means for authenticated clients for accessing desired web sites hosted by various servers throughout a network. For example, the system can establish a two-way trusted (secured) communications link between authenticated users (shoppers) and various e-Commerce merchants, in which, the authenticity of the message and identity of the shopper (sender) would be validated by the merchant, as taught by Ramasubramani et al (see column 4, lines 18-28.)

As to claim 10, Reed et al as modified teaches wherein the identifying step includes: providing session parameters for each of the identified clients for at least one of the application servers (see Reed et al, column 34, lines 18-47, and see Ramasubramani et al, column 14, lines 18-30, where “session parameters” is read on “device ID in the session request”).

As to claim 11, Reed et al as modified teaches wherein the identifying step includes: providing a user interface to the identified clients for accessing the application servers (see Reed et al, column 68, lines 9-13, and see Ramasubramani et al, column 9, lines 29-32.)

As to claim 13, Reed et al as modified teaches wherein the user interface includes a listing of application servers (see Ramasubramani et al, Abstract, where “listing of application servers” is read on “plurality of secure servers”, and see column 7, lines 41-45,

Art Unit: 2165

where “list of application servers” is read on “certain web servers”) and the establishing step is initiated following a selection of an application server by a user from the user interface (see Reed et al, column 26, lines 47-64.)

As to claim 14, Reed et al as modified teaches the method further comprising a plurality of application servers connected to the network (see Ramasubramani et al, Abstract, where “listing of application servers” is read on “plurality of secure servers”, and see column 7, lines 41-45, where “list of application servers” is read on “certain web servers”), each requiring authentication for access (see Reed et al, column 153, lines 20-23, and see Ramasubramani et al, column 7, lines 41-45.)

***Allowable Subject Matter***

4. Claim 3 and 12 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.
5. Claim 5 is objected to as a dependent of the objected to dependent claim 3.

***Response to Arguments***

6. Applicant's arguments filed on 23-September-2005 with respect to the rejected claims in view of the cited references have been fully considered but they are not deemed persuasive:

In response to the applicant's arguments that "Ramasubramani does not disclose or suggest such an authenticated link", the arguments have been fully considered but are not deemed persuasive, because "authenticated link" is not recited in the rejected claim.

Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Rejected independent claims 1 and 9 recite the limitation, "establishing a two-way trusted communication link" which is taught by Ramasubramani et al. The "two way communication" is taught in column 3, lines 20-22 and in column 5, lines 3-5, and "trusted" is taught in column 6, lines 34-38 of Ramasubramani et al, where "trusted" is read on "secure and authenticated communications".

In response to the applicant's arguments that "Ramasubramani does not disclose or suggest an authentication server that establishes a two-way trusted communication link", the arguments have been fully considered but are not deemed persuasive, because such "two-way trusted" communication link is taught by Ramasubramani et al, as explained above, and further, the "authentication server" is taught by Ramasubramani et al in column 4, lines 9-28, where "authentication server" is read on "the authentication process using the digital IDs between the client and the merchant server".

Art Unit: 2165

***Conclusion***

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiries concerning this communication or earlier communications from the examiner should be directed to Tony Mahmoudi whose telephone number is (571) 272-4078. The examiner can normally be reached on Mondays-Fridays from 08:00 am to 04:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Gaffin, can be reached at (571) 272-4146.

tm

November 30, 2005

  
JEFFREY GAFFIN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100